CVE-2017-12615

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-12615
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-19 13:29:00 UTC
Updated	2026-04-21 17:04:04 UTC
Description	When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisat

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.941980000 probability, percentile 0.999210000 (date 2026-04-21)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Known

Problem Types: CWE-434 | Remote Code Execution | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

CISA Known Exploited Vulnerability

Vendor	Apache
Product	Tomcat
Name	Apache Tomcat on Windows Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-12615

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Application	Apache	Tomcat	All	All
Operating System	Microsoft	Windows	-	All
Application	Netapp	7-mode Transition Tool	-	All
Application	Netapp	Oncommand Balance	-	All
Application	Netapp	Oncommand Shift	-	All

Operating System	Redhat	Enterprise Linux Desktop	6.0	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All
Operating System	Redhat	Enterprise Linux Eus Compute Node	7.4	All
Operating System	Redhat	Enterprise Linux Eus Compute Node	7.5	All
Operating System	Redhat	Enterprise Linux Eus Compute Node	7.6	All
Operating System	Redhat	Enterprise Linux Eus Compute Node	7.7	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems	7.0_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.4_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.5_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.6_s390x	All
Operating System	Redhat	Enterprise Linux For Ibm Z Systems Eus	7.7_s390x	All
Operating System	Redhat	Enterprise Linux For Power Big Endian	7.0_ppc64	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.4_ppc64	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.5_ppc64	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.6_ppc64	All
Operating System	Redhat	Enterprise Linux For Power Big Endian Eus	7.7_ppc64	All
Operating System	Redhat	Enterprise Linux For Power Little Endian	7.0_ppc64le	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.4_ppc64le	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.5_ppc64le	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.6_ppc64le	All
Operating System	Redhat	Enterprise Linux For Power Little Endian Eus	7.7_ppc64le	All
Operating System	Redhat	Enterprise Linux For Scientific Computing	7.0	All
Operating System	Redhat	Enterprise Linux Server	6.0	All
Operating System	Redhat	Enterprise Linux Server	7.0	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	7.4_ppc64le	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	7.6_ppc64le	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	7.7_ppc64le	All
Operating System	Redhat	Enterprise Linux Server For Power Little Endian Update Services For Sap Solutions	9.2_ppc64le	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All

Operating System	Redhat	Enterprise Linux Server Tus	7.6	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All
Application	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.4	All
Application	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.6	All
Application	Redhat	Enterprise Linux Server Update Services For Sap Solutions	7.7	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All
Application	Redhat	Jboss Enterprise Web Server	2.0.0	All
Application	Redhat	Jboss Enterprise Web Server	3.0.0	All
Application	Redhat	Jboss Enterprise Web Server Text-only Advisories	-	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Tomcat	affected 7.0.0 to 7.0.79	Not specified

References

Reference
Red Hat Customer Portal
GitHub - breaktoprotect/CVE-2017-12615: POC Exploit for Apache Tomcat 7.0.x CVE-2017-12615 PUT JSP vulnerability.
Red Hat Customer Portal
www.cisa.gov/known-exploited-vulnerabilities-catalog
Red Hat Customer Portal
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)
Apache Tomcat CVE-2017-12615 Remote Code Execution Vulnerability
Break To Protect: The Case of CVE-2017-12615 Tomcat 7 PUT vulnerability
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Red Hat Customer Portal
Synology-SA-17:54 Tomcat | Synology Inc.
Apache Tomcat on Windows HTTP PUT Request Processing Flaw Lets Remote Users Execute Arbitrary Code on the Target System - Securit
Pony Mail!
Pony Mail!
August 2017 Apache Tomcat Vulnerabilities in NetApp Products | NetApp Product Security

Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-25T00:00:00.000Z	CVE-2017-12615 added to CISA KEV

Legacy QID Mappings

378318 Virtuozzo Linux Security Update for tomcat6-lib (VZLSA-2017:3080)

980957 Java (maven) Security Update for org.apache.tomcat.embed:tomcat-embed-core (GHSA-pjfr-qf3p-3q25)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**